

AN 2003-134037 [13] WPIDS

DNN N2003-106729 [13]

TI Apparatus authorization system e.g. for mobile telephone, attests wireless card based on certification information received from card, for operating mobile telephone

DC T01; W01

IN KAMAYA Y; NAKAKITA H

PA (TOKE-C) TOSHIBA KK

CYC 1

PI JP 2002366529 A 20021220 (200313)* JA 20[23]

ADT JP 2002366529 A JP 2001-171602 20010606

PRAI JP 2001-171602 20010606

IPCR G06F0015-00 [I,A]; G06F0015-00 [I,C]; G06F0021-20 [I,A]; G06F0021-20 [I,C]; H04L0009-32 [I,A]; H04L0009-32 [I,C]; H04Q0007-38 [I,A]; H04Q0007-38 [I,C]

AB JP 2002366529 A UPAB: 20050528

NOVELTY - Certification information for controlling operation of mobile telephone (20a), is generated by wireless card (10) and is transmitted to the mobile telephone. The mobile telephone is operated only when the card is attested based on the received certification information.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for apparatus certification method.

USE - For certifying wireless card to control operation of mobile telephone, PC, vehicle, etc., by user.

ADVANTAGE - Decoding of certification information by third person is prevented, hence safety of mobile telephone, PC, etc., is ensured.

DESCRIPTION OF DRAWINGS - The figure shows the structure of apparatus authorization system. (Drawing includes non-English language text).

Wireless card (10)

Mobile telephone (20a)

MC EPI: T01-J; W01-A05B; W01-B05A

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-366529

(P2002-366529A)

(43) 公開日 平成14年12月20日 (2002. 12. 20)

| (51) Int.Cl. ⁷ | 識別記号 | F I | テームコード* (参考) |
|---------------------------|-------|---------------|-------------------|
| G 0 6 F 15/00 | 3 3 0 | G 0 6 F 15/00 | 3 3 0 G 5 B 0 8 5 |
| | | | 3 3 0 C 5 J 1 0 4 |
| H 0 4 L 9/32 | | H 0 4 L 9/00 | 6 7 5 A 5 K 0 6 7 |
| H 0 4 Q 7/38 | | H 0 4 B 7/26 | 1 0 9 R |

審査請求 未請求 請求項の数10 O L (全 20 頁)

(21) 出願番号 特願2001-171602(P2001-171602)

(22) 出願日 平成13年6月6日(2001. 6. 6)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 中北 英明

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(72) 発明者 釜谷 幸男

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(74) 代理人 100083806

弁理士 三好 秀和 (外7名)

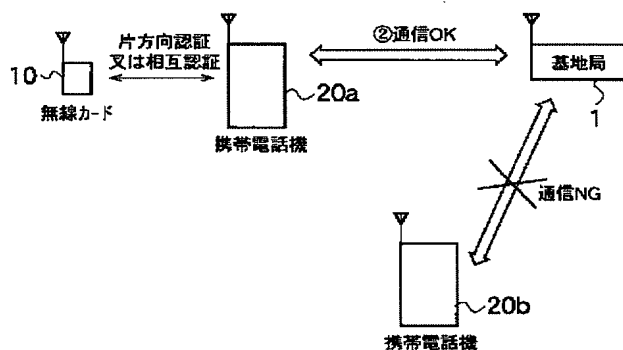
最終頁に続く

(54) 【発明の名称】 機器認証システム及び機器認証方法

(57) 【要約】

【課題】 電子機器（例えば、携帯電話機20）を使用する際に、利用者が所有する無線カード10を用いて、その無線カード20と電子機器との間で認証を行うことにより、その電子機器の使用を可能とするものである。

【解決手段】 電子機器（例えば、携帯電話機20）の動作を制御するための認証を行う機器認証システムであって、電子機器の動作を制御するための認証情報を生成する第一認証部と、第一認証部で生成した認証情報を電子機器に送信する送信手段とを有する無線カード10とを有し、電子機器は、認証情報を無線カード10から受信する受信手段と、受信手段が受信した認証情報に基づいて無線カード10の認証を行う第二認証部と、第二認証部の認証に基づいて電子機器を動作させる動作制御部とから概略構成される。



(2)

1

【特許請求の範囲】

【請求項1】 電子機器の動作を制御するための認証を行う機器認証システムであって、前記電子機器の動作を制御するための認証情報を生成する第一認証部と、前記第一認証部で生成した認証情報を前記電子機器に送信する送信手段とを有する無線カードとを有し、前記電子機器は、前記認証情報を前記無線カードから受信する受信手段と、前記受信手段が受信した前記認証情報に基づいて前記無線カードの認証を行う第二認証部と、前記第二認証部の認証に基づいて前記電子機器を動作させる動作制御部とを有することを特徴とする機器認証システム。

【請求項2】 請求項1に記載の機器認証システムであって、前記電子機器は、前記認証情報を前記無線カードから取得するために、前記認証情報を要求する認証要求情報を生成する認証情報要求部と、前記認証要求情報を前記無線カードに対して送信する送信手段とを有することを特徴とする機器認証システム。

【請求項3】 請求項2に記載の機器認証システムであって、前記電子機器は、操作手段に対する操作を検知する検知部を有し、前記認証情報要求部は、前記検知部での検知に基づいて、前記無線カードに対して前記認証情報を要求することを有することを特徴とする機器認証システム。

【請求項4】 請求項1又は請求項2に記載の機器認証システムであって、前記送信手段は、前記受信手段に対して、前記受信手段と同じ通信条件を用いて、前記受信手段を呼び出し、その呼び出しに応じた前記受信手段と通信接続をした後に前記認証情報又は前記認証要求情報を送信することを特徴とする機器認証システム。

【請求項5】 通信方式としてBluetooth方式を使用したことを特徴とする請求項4に記載の機器認証システム。

【請求項6】 請求項2乃至請求項5に記載の機器認証システムであって、前記認証情報要求部は、前記認証要求情報を所定の時間毎に要求するようにするための要求時間を設定する設定手段を有することを特徴とする機器認証システム。

【請求項7】 電子機器の動作を制御するための認証を行う機器認証方法であって、無線カードにおいて、前記電子機器の動作を制御する認証情報を生成し、その生成された前記認証情報を前記電子機器に送信するステップと、前記電子機器において、前記無線カードから送信された認証情報を受信し、その受信した前記認証情報を認証し、その認証に基づいて前記電子機器を動作させるステップとを有することを特徴とする機器認証方法。

2

【請求項8】 請求項7に記載の機器認証方法であって、

前記電子機器において、前記認証情報を前記無線カードから受信するために、前記認証情報を要求する認証要求情報を前記無線カードに対して送信するステップと前記無線カードにおいて、前記認証要求情報を前記電子機器から受信し、その受信した前記認証要求情報に基づいて、前記認証情報を生成するステップとを有することを特徴とする機器認証方法。

10 【請求項9】 請求項8に記載の機器認証方法であって、前記電子機器において、操作手段の操作を検知するステップと、その検知に基づいて前記認証要求情報を前記無線カードに対して送信するステップとを有することを特徴とする機器認証方法。

【請求項10】 請求項8又は請求項9に記載の機器認証方法であって、前記電子機器において、前記認証要求情報を所定の時間毎に要求するための時間を設定するステップと、前記設定された時間に基づいて、前記無線カードに対して前記認証要求情報を送信するステップとを有することを特徴とする機器認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子機器の動作を制御するための認証を行う機器認証システム及び機器認証方法に関する。

【0002】

30 【従来の技術】近年のLAN (Local Area Network) 技術の発達に伴い、オフィス環境では、PC (Personal Computer) 間の接続を中心として、ネットワーク化が進行している。また、有線LANのみではなく、有線LANの一部分を無線で置換する無線LAN化も進んでいる。例えば、有線LANに無線基地局を接続し、この無線基地局に複数のパーソナルコンピュータを無線で接続する無線LANが挙げられる。即ち、基地局と携帯型PCとの部分だけを見ても、その部分は無線LANを形成しているものである。この無線LANを用いることは、伝送路として電波や赤外線などの無線通信技術を利用することになるので、配線敷設が不要となり、ネットワークの新設やレイアウト変更を容易に行うことができる。

40 【0003】一方、このような無線通信技術の中でも特に注目されているのが、10m程度の近接距離のアドホックネットワークを構成することを対象としたBluetooth (以下、単に「BT」と略す) である。このBTは、通信速度が1Mbps程度、IrDaのような指向性はもたないなどの特徴がある。また、BTは、近い将来、1チップ5ドル程度という低コストで実現されようとしており、携帯電話業界、家電業界、更にPC業界を巻き込む

50

(3)

3

だ幅広い業種の約2000社が標準化団体に参加している。そのため、BTを搭載した様々な無線機器が今後世界的に普及すると予想される。

【0004】

【発明が解決しようとする課題】しかしながら、BTなどの無線機器は、ケーブル接続などの場合のように明示的な接続ではないので、セキュリティやプライバシーの保護が問題となりやすい。また、携帯性の高い機器は、落としやすいなどといった管理上の問題もあるので、前記機器を落としてしまった場合であっても、第三者に前記機器を使用できなくさせるようにするための方法が必要であった。

【0005】そのため、従来から携帯電話機の場合には、図23に示すように携帯電話機にパスワードを設定する機能を持たせており、他人に拾得され、又は、盗難されても、ある程度は携帯電話機を使用できなくさせることが可能であった。しかし、現実には、無線機器のユーザは、パスワード設定をあまり行っていないのが現状であり、また、パスワード設定がされていたとしても、銀行カードの場合のように、一旦パスワード設定すれば二度と変更する必要のないものとして一般的には認識されているものであった。

【0006】したがって、パスワードを設定し、かつ、頻繁に変更している一般ユーザは、それほど多くはないものと考えられ、パスワード設定されていない携帯電話機が第三者に盗難等されてしまった場合には、第三者に不当な携帯電話機の使用がされる可能性があった。又、パスワード設定されていたとしても、パスワードの桁数が小さければ、総当たり攻撃などによってパスワードが簡単に破られてしまう恐れがある。

【0007】そこで、本発明は以上の点に鑑みてなされたもので、電子機器を使用する際に、利用者の無線カードにより認証を行わなければ、その電子機器を使用することができないようにし、また、無線カード内にある特有の認証情報を、第三者に容易に解読させないようにするための機器認証システム及び機器認証方法を提供することを課題とする。

【0008】

【課題を解決するための手段】本発明に係る発明は上記課題を解決すべくなされたものであり、請求項1に係る発明は、電子機器の動作を制御するための認証を行う機器認証システムであって、前記電子機器の動作を制御するための認証情報を生成する第一認証部と、前記第一認証部で生成した認証情報を前記電子機器に送信する送信手段とを有する無線カードとを有し、前記電子機器は、前記認証情報を前記無線カードから受信する受信手段と、前記受信手段が受信した前記認証情報に基づいて前記無線カードの認証を行う第二認証部と、前記第二認証部の認証に基づいて前記電子機器を動作させる動作制御部とを有することを特徴とするものである。

4

【0009】このような請求項1に係る発明によれば、無線カード側で生成された電子機器の動作を制御するための認証情報を電子機器が取得することにより、その取得した認証情報に基づいて電子機器を動作させることができる。そのため、電子機器で取得した認証情報が適正な情報でない場合には、前記電子機器を動作させることができず、適正な認証情報を持った者のみが電子機器を動作させることができる。

【0010】また、電子機器は、無線カード（適正な認証情報が格納されたもの）を有する者のみしか使用できないことになるので、前記電子機器を盗難され、又は、紛失した場合であっても、その盗難した者等に使用されないようにすることができる。

【0011】請求項2に係る発明は、請求項1に記載の機器認証システムであって、前記電子機器は、前記認証情報を前記無線カードから取得するために、前記認証情報を要求する認証要求情報を生成する認証情報要求部と、前記認証要求情報を前記無線カードに対して送信する送信手段とを有することを特徴とするものである。

【0012】このような請求項2に係る発明によれば、電子機器の所有者は、電子機器を使用する際に、無線カードに対して電子機器を動作させるための認証情報を要求することができるので、電子機器の通信可能範囲内に無線カードがあれば、無線カードを持ち歩かなくても電子機器を動作させるための認証情報を無線カードから容易に取得することができる。

【0013】請求項3に係る発明は、請求項2に記載の機器認証システムであって、前記電子機器は、操作手段に対する操作を検知する検知部を有し、前記認証情報要求部は、前記検知部での検知に基づいて、前記無線カードに対して前記認証情報を要求することを有することを特徴とするものである。

【0014】このような請求項3に係る発明によれば、電子機器の利用者が電子機器を使用する際に、電子機器側の操作により無線カードに対して認証情報を要求するので、無線カード側で特別な操作をしなくても無線カードと電子機器との間で認証を行うことができる。

【0015】請求項4に係る発明は、請求項1又は請求項2に記載の機器認証システムであって、前記送信手段は、前記受信手段に対して、前記受信手段の周波数とクロックのタイミングにより、前記受信手段を呼び出し、その呼び出しに応じた前記受信手段と通信接続をした後に前記認証情報又は前記認証要求情報を送信することを特徴とするものである。

【0016】このような請求項4に係る発明によれば、送信手段は、受信手段に対して、その受信手段が有する特定の周波数とクロックのタイミングにより受信手段との間で通信接続を確立させることができるので、例えば、近接無線通信を行うBT (Bluetooth) によって通信接続を確立させることができる。

(4)

5

【0017】請求項5に係る発明は、通信方式としてBluetooth方式を使用したことを特徴とする請求項4に記載の機器認証システムである。

【0018】このような請求項5に係る発明によれば、無線カードと電子機器との間の通信方式としてBluetooth方式を用いることができるので、通信速度が速く、相対的姿勢に自由度をもった通信をすることが可能となる。

【0019】請求項6に係る発明は、請求項2乃至請求項5に記載の機器認証システムであって、前記認証情報要求部は、前記認証要求情報を所定の時間毎に要求するようにするための要求時間を設定する設定手段を有することを特徴とするものである。このような請求項6に係る発明によれば、無線カードと電子機器との間の認証を所定の時間毎に行うので、無線カードを所持した利用者が電子機器から離れてしまい無線カードと電子機器との間で認証ができなくなった場合には、電子機器の動作を停止させることができる。そのため、第三者に電子機器のみが盗難された場合には、その盗難された電子機器と共通の認証情報を有する無線カードとの間で認証を行うことができないので、第三者に盗難された電子機器を不当に使用されることがなくなる。

請求項7に係る発明は、電子機器の動作を制御するための認証を行う機器認証方法であって、無線カードにおいて、前記電子機器の動作を制御する認証情報を生成し、その生成された前記認証情報を前記電子機器に送信するステップと、前記電子機器において、前記無線カードから送信された認証情報を受信し、その受信した前記認証情報を認証し、その認証に基づいて前記電子機器を動作させるステップとを有することを特徴とするものである。

【0020】このような請求項7に係る発明によれば、無線カード側で生成された電子機器の動作を制御するための認証情報を電子機器が取得することにより、その取得した認証情報に基づいて電子機器を作動させることができる。そのため、電子機器で取得した認証情報が適正な情報でない場合には、前記電子機器を作動させることができず、適正な認証情報を持った者のみが電子機器を作動させることができる。

【0021】請求項8に係る発明は、請求項7に記載の機器認証方法であって、前記電子機器において、前記認証情報を前記無線カードから受信するために、前記認証情報を要求するための認証要求情報を前記無線カードに対して送信するステップと、前記無線カードにおいて、前記認証要求情報を前記電子機器から受信し、その受信した前記認証要求情報に基づいて、前記認証情報を生成するステップとを有することを特徴とするものである。

【0022】このような請求項8に係る発明によれば、電子機器が無線カードに対して認証情報を要求するので、無線カード側で特別な操作をしなくても無線カード

6

と電子機器との間で認証を行うことができる。

【0023】請求項9に係る発明は、請求項8に記載の機器認証方法であって、前記電子機器において、操作手段の操作を検知するステップと、その検知に基づいて前記認証要求情報を前記無線カードに対して送信するステップとを有することを特徴とするものである。

【0024】このような請求項9に係る発明によれば、電子機器の利用者が電子機器を使用する際に、電子機器からの操作により無線カードに対して認証情報を要求するので、無線カード側で特別な操作をしなくても無線カードと電子機器との間で認証を行うことができる。

【0025】請求項10は、請求項8又は請求項9に記載の機器認証方法であって、前記電子機器において、前記認証要求情報を所定の時間毎に要求するための時間を設定するステップと、前記設定された時間に基づいて、前記無線カードに対して前記認証要求情報を送信するステップとを有することを特徴とするものである。

【0026】このような請求項10に係る発明によれば、電子機器が無線カードに対して設定された時間毎に認証要求情報を要求することにより、無線カードと電子機器との間の認証を行うので、無線カードを所持した利用者が電子機器から離れてしまい無線カードと電子機器との間で認証ができなくなった場合には、電子機器の動作を停止させることができる。そのため、無線カードを所持している利用者が電子機器から離れている間は、第三者に電子機器を使用させないようにすることができる。

【0027】

【発明の実施の形態】（機器認証システムの構成）本発明の実施形態について図面を参照しながら説明する。図1は、本実施形態に係る機器認証システムの概略構成図である。

【0028】同図に示すように、本実施形態に係る機器認証システムは、主に、無線カード10と携帯電話機20aとから構成されており、無線カード10と携帯電話機20aとの間の認証が成功した場合のみ携帯電話機20aを管理する基地局1と通信をすることができる。そのため、無線カード10との間で認証が行われていない携帯電話機20bは、基地局1と通信することができない。

【0029】図2は、図1に示す無線カード10と携帯電話機20との間の認証方法を示したものである。同図に示すように、無線カード10と携帯電話機20には、両者に共通の秘密鍵SA1及び暗号アルゴリズムCA1が予め共有されている。例えば、この秘密鍵SA1及び暗号アルゴリズムは製造時に埋め込むことができる。

【0030】無線カード10には、乱数生成装置があり、乱数Aを生成する。この乱数Aは、無線カード10から携帯電話機20へと送信される。その乱数Aなどを受信した携帯電話機20は、秘密鍵SA1及び暗号アルゴ

(5)

7

リズムCA1によって暗号化する。そして、携帯電話機20では、この暗号化された結果を応答として無線カード10へと返信する。その後、無線カード10側では、乱数Aを秘密鍵SA1と暗号アルゴリズムCA1で暗号化したものを持ち、この応答と比較することによって認証の可否を判断する。この認証判断は、無線カード10が携帯電話機20の秘密鍵SA1及び暗号アルゴリズムCA1により認証判断するので、片方認証といわれる。尚、図2とは逆方向の片方認証もあり得る。

【0031】図3は、無線カード10と携帯電話機20との間で行われる認証を相互から行ったことを示したものである。具体的には、同図に示すように、無線カード10が携帯電話機20の認証を行うだけでなく、携帯電話機20の方からも無線カード10の認証を行うものである。この無線カード10と携帯電話機20との間で相互の認証が成功し場合には、携帯電話機20と基地局1との間で通信を行うことができる。

【0032】これらの認証の確立は、操作性という面からはできるだけ短時間で終了するのが望ましい。また、このような認証用の無線カード10は、携帯可能という点から、できるだけ小型で、且つ、普及を考えると低価格という要求条件がある。

【0033】図4は、無線カード10と携帯電話機20との間で行われる認証を近接無線通信（本実施形態では、Bluetooth（以下単に「BT」と略す）を用いるものとする）を用いて認証したことを示したものである。具体的には、同図に示すように、先ず、製造時や出荷などに、認証情報（PINコードなど）を管理しているホストシステム30が両者に共通のPINコードを無線カード10と携帯電話機20に格納させる。その後、無線カード10又は携帯電話機20から両者に共通のPINコードや、乱数A又は乱数Bを送信させることで、両者に共通の認証情報を生成させて、その生成させた認証情報に基づいて無線カード10と携帯電話機20との間で認証を行う（詳述は後述する）。

【0034】そして、その認証が成功した場合には、携帯電話機20と基地局1との間で通信を行うことができる。本実施形態では、無線カード10と携帯電話機20との認証は、BTを用いて行うものとする。

【0035】図5は、本実施形態に係る機器認証システムの内部構造を示すブロック図を示したものであり、本実施形態に係る機器認証システムは、ホストシステム30と、無線カード10、携帯電話機20とを有している。

【0036】前記ホストシステム30は、無線カード10又は携帯電話機20を管理するものであり、パーソナルコンピュータ等が挙げられる。本実施形態では図5に示すように、ホストシステム30内のシステム全体の制御を司るCPU31と、CPU31が実行する制御プログラムを格納したROM32と、情報記録領域を備えた

8

RAM33と、無線カード10との間で情報データの送受信をする通信I/F34と、情報データの内容を表示させる表示部37と、情報データを入力する操作部36とを有している。

【0037】このホストシステム30は、無線カード10及び携帯電話機20を製造する際に、両者に共通のコード情報（例えば、PINコードなど）を無線カード10にあるインターフェース（図示せず）（又は通信I/F34）を介してRAM13及びRAM23に格納する（図5参照）。ここで、コード情報は、認証情報を生成させるための情報であり、本実施形態では、図6に示すように、任意に発生された乱数（128ビットのもの）、PINコード、PINコード長、暗証番号などが挙げられる。

【0038】尚、ホストシステム30は、例えば、工場内、又は、携帯電話機20を販売している販売店、若しくは、代理店などに設置されているものである。従って、ホストシステム30内でネットワークが構成されて、認証情報の分散管理がなされていればよい。

【0039】表示部37は、情報データを表示させる表示手段であり、例えば、液晶画面などが挙げられる。この情報データは、例えば、文字データ、画像データ、動画データ、コード情報、認証情報などが挙げられる。具体的に表示部37は、CPU31からの命令により、記憶装置35で格納されているコード情報を表示させるものである。また、表示部37は、コード情報を通信I/F34を介して無線カード10に送信した場合には、表示部37にある画面表示部に”コード情報は、〇〇〇の無線カード10に送信しました”などの表示をさせることもできる。

【0040】操作部36は、情報データを入力し、表示部37にある画面表示を操作する操作手段であり、例えば、キーボードなどが挙げられる。尚、操作部36の形状としては、ボタン形状のものや、ジョイスティック型のものが挙げられる。

【0041】通信I/F34は、無線カード10又は携帯端末機20との間で情報データの送受信をするものであり、例えば、BT、IrDA端末などが挙げられる。ここで、BTとは、周波数ホッピング型のスペクトル拡散方式を用いてデータ通信を行うものである（詳しくは後述する）。また、IrDAとは、赤外線を利用してデータ通信を行うものである。

【0042】記憶装置35は、認証情報を格納するものであり、例えば、ハードディスク装置などが挙げられる。また、この記憶装置35で蓄積するコード情報としては、PINコードなどが挙げられる。具体的に記憶装置35は、図7に示すように、携帯電話機20毎に定められたPIN1～PINnを格納している。

【0043】前記無線カード10は、本実施形態では、電子機器の動作を制御するための認証情報を生成する第

(6)

9

一認証部と、第一認証部で生成した認証情報を電子機器に送信する送信手段とを有するものであり、本実施形態では同図に示すように、無線カード10内のシステム全体の制御を司るCPU11と、CPU11が実行する制御プログラムを格納したROM12と、無線カード10と携帯端末機20との間で認証を行うための認証情報を記録するコード情報領域13aを備えたRAM13と、ホストシステム30と携帯端末機20との間で情報データの送受信をする通信I/F14と、情報データの内容を表示させる表示部15と、情報データを入力する操作部16とを有している。

【0044】尚、この無線カード10の形状としては、カード状又はキーホルダー状のようなものが挙げられる。また、無線カード10は、携帯電話機20とセットで販売することができるものである。更に、無線カード10は、携帯電話機20と有線によって接続できるものであっても、また、携帯電話機20のカードスロットに挿入する形式であってもよい。

【0045】表示部15は、情報データを表示させるものであり、例えば、液晶画面などが挙げられる。この情報データは、例えば、文字データ、画像データ、動画データなどが挙げられる。具体的に表示部15は、CPU11からの命令により、通信I/F14で受信した情報データを表示させるものである。例えば、無線カード10と携帯電話機20との間で適正な認証が行われた場合には、表示部15は、CPU11からの命令により適正な認証が行われた旨の表示（例えば、“携帯電話機との認証は終了しました”。）をすることができる。

【0046】操作部16は、情報データを入力し、表示部15にある画面表示を操作するものであり、例えば、キーボードなどが挙げられる。尚、操作部16の形状としては、ボタン形状のものや、ジョイスティック型のものが挙げられる。

【0047】RAM13は、電子機器の動作を制御するための認証情報を生成する第一認証部であり、本実施形態では、認証情報を生成するためのコード情報が格納されているコード情報記録領域13aを有している。このコード情報領域13aに格納されるコード情報としては、図6に示すように、128ビットで構成されている任意のコードである乱数、PINコード（Personal Identification Number）、PINコード長などが記録されている。このPINコードを記録する際には、外部から容易に書き替えられないようにした形式（プロテクターをかける）で格納することができる。

【0048】このプロテクターをかけてRAM13にPINコードを格納した場合に、その無線カード10を紛失したときには、例えば、携帯電話機20を製造工場又は販売店に持ち込んで、その製造工場又は販売店にあるホストシステム30で以前格納してあったPINコードとは別のPINコードを設定する。これにより、無線カ

10

ード10を紛失したとしても、PINコードを容易に書き替えることができないので、その紛失した携帯電話機20を他の者によって使用させないようにすることができる。また、このとき、以前のPINコードは、ホストシステム30で使用不可として管理可能である。

【0049】一方、このPINコードは、無線カード10の使用者が操作部16を介して自由に設定させるようにすることもできる。例えば、無線カード10の使用者が操作部16でPINコードの長さを変更したり、又は、PINコードを定期的に変更させたりすることができる。これにより、認証情報（PINコードなど）を変更（定期的に）することができるので、無線カード10と携帯電話機20の間で行うデータ送受信の際のセキュリティレベルを自由に設定することができる。

【0050】また、無線カード10と携帯電話機20との間でしか情報データを交信することができないようにするための秘密鍵（図示せず）や、操作部16の操作により、暗証番号（例えば“1234”などの情報）も認証情報として用いることで、無線カード10と携帯電話機20の間でデータの送受信を行う際のセキュリティレベルを更に上げることができる。

【0051】通信I/F14は、ホストシステム30と通信I/F14との間で情報データの送受信をするものであり、例えば、BT、IrDAなどが挙げられる。本実施形態で通信I/F14は、第一認証部で生成した認証情報を電子機器（例えば、携帯電話機20）に送信する送信手段を有する送信部14aと、認証情報を要求するための認証要求情報を携帯電話機20から受信する受信手段を有する受信部14bと、無線カード10で生成された認証情報と携帯電話機20で生成された認証情報とが一致しているか否かを判断する認証部14cとを有している。

【0052】BTの場合は、送信部14aは、受信手段（本実施形態では、携帯電話機20の受信部24b）に対して、前記受信手段の周波数とクロックのタイミングにより、前記受信手段を呼び出し、その呼び出しに応じた前記受信手段と通信接続をした後に認証情報又は認証要求情報を送信する。

【0053】このBT I/Fでは、通信可能な範囲内にある携帯電話機20との接続可能性の向上等のために、待ち受け側のBT I/Fが接続要求を監視する周波数（待ち受け周波数）を所定時間毎に変化させている。

【0054】この待ち受け周波数の変化パターンは、待ち受け側のBT I/Fに割り当てられた識別情報（BT-AD（Address）、BT-CLK（Clock））によって異なるが、通常、通信を開始しようとするときには、通信可能な範囲内に存在するBT I/Fの識別情報（特にBT-AD）が不明である。このため、通信を開始しようとする送信部14aは、まず、周囲のBT I/Fを検出するための問い合わせ（Inquiry）処理によって、自機

(7)

11

の周囲に存在するBT I/Fを検出する。

【0055】このInquiryの要求に応じて、周囲のBT I/Fからの応答を受信部14bが受信すると、この応答中のBT-ADに応じて通信しようとするBTを選択し、呼び出し(Page)処理によって、選択した相手呼び出す。このPageにより、相手側のBT送受信機が提供しているサービスを検出すると、所定のサービスを指定して、通信接続モードに移行し、接続を確立する。

【0056】この無線カード10と携帯電話機20との間で通信接続が確立した後に、携帯電話機20にある送信部24a・受信部24bと無線カード10にある送信部14a・受信部14bとの間で認証情報が送受信されて、認証部14c及び認証部24cで認証が行われる(詳細は後述する)。

【0057】このBTを通信方式として用いることにより、鞆の中に無線カード10を入れておいたり、又は、無線カード10を携帯電話機20に付けて携帯したりするというような利用形態で、無線カード10と携帯電話機20との間で簡単に認証処理をすることができる。そのため、無線カード10を所有した者のみしか携帯電話機20を使用することができなくなるので、携帯電話機20を他の者によって許可なく使用されることがなくなり、携帯電話機20を利用する際の安全性を高めることができる。

【0058】認証部14cは、無線カード10で生成された認証情報と携帯電話機20で生成された認証情報とが一致しているか否かを判断するものである。この認証部14cで行う認証は、上述の如く、BTで通信接続が確立された後に行われるものである。ここで認証情報としては、後述するリンクキーが挙げられる。

【0059】この認証部14cで行われる認証は、認証情報(リンクキー)によって定められる。ここでリンクキーとは、ある2つのBT I/F間において、1対1関係をセキュアに管理する共通パラメータのことをいうものである。

【0060】セキュアに認証は、無線カード10をマスター、携帯電話機20をスレーブとして、ピコネットを形成してから行われ、この認証が成功したときのみ携帯電話機20の使用が可能となる。ここでBTの認証情報(リンクキー)としては、初期化キーKin、単体キーKa、複合キーKabのいずれかが使用されるが、それぞれ128ビットの固有長を有する。

【0061】以下、認証部14cで行われるリンクキー(初期化キーKin、単体キーKa、複合キーKab)の生成と、そのリンクキーを用いて無線カード10と携帯電話機20との間で行われる認証について説明する。

【0062】初期化キーKinの生成について図面を参照しながら説明する。図8は、初期化キーKinを生成するまでのブロック図を示したものである。また、図9は、初期化キーKinが生成されるまでの詳細なフロー図を示

12

したものである。この初期化キーKinは、無線カード10と携帯端末機20とにあるBT I/F間で初めて接続を試みるときに使用されるリンクキーをいうものである。

【0063】また、初期化キーKinは、後述する単体キーKa又は複合キーKabに置き換えられる一時的なキーではあるが、その単体キーKa又は複合キーKabが生成されるまでは初期化キーKinを保持しておき、認証の際に常に使用されるものである。

【0064】図8に示すように、初期化キーKinの生成は、任意のコードである乱数1と、PIN1と、PINコード長とを、それぞれ無線カード10と携帯電話機20とにある認証部14c及び認証部24cに入力させる。そして、認証部14c及び認証部24cにある関数[E22]は、入力された乱数1、PIN1、PINコード長とに基づいて初期化キーKinを生成させる。この関数[E22]は、BT I/Fに内蔵されているもので、初期化キーKinを生成するためのアルゴリズムを意味するものである。

【0065】この初期化キーKinを生成するまでのフローについて図9を参照しながら説明する。同図に示すように、先ず、認証部14cが、RAM13からPIN1と、乱数1と、PINコード長とを読み込むことを行う(S101a)。一方、認証部24cは、RAM23からPIN1及びPINコード長を読み込むことを行う(S101b)。

【0066】そして、無線カード10の送信部14aを介して、携帯電話機20に乱数1を送信し、その送信された乱数1を携帯電話機20で受信する(S102a、S102b)。尚、無線カード10及び携帯電話機20に共通のPIN1は、無線カード10と携帯電話機20の製造工程でRAM13及びRAM23に予め格納しておく。

【0067】その後、認証部14cは、PIN1と、PINコード長、乱数1に基づいて初期化キーKinを関数[E22]で生成させて(S103a)、その生成させた初期化キーKinをRAM13に格納させる。

【0068】一方、認証部24cは、PIN1と、PINコード長と、無線カード10から送信されてきた乱数1に基づいて関数[E22]で初期化キーKinを生成させて(S103b)、その生成させた初期化キーKinをRAM23に格納させる。これにより、無線カード10と携帯電話機20との間で共通の初期化キーKinを所有させることができる。

【0069】単体キーKaの生成について図面を参照しながら説明する。図10は、単体キーKaを生成するまでのブロック図を示したものである。また、図11は、単体キーKaを生成するまでの詳細なフロー図を示したものである。この単体キーKaは、BTで恒久的に用いられるリンクキーをいうものであり、初期化キーKinを生成した後に生成されるものである。この単体キーKaにより、どのBT I/Fに対しても自分の単体キーKaをリンクキー

(8)

13

として用いることができるので、接続相手毎にリンクキーをデータベースで管理する必要がなくなる。

【0070】図10に示すように、無線カード10側での単体キーKaの生成は、先ず、乱数2と無線カード10のBT-AD1とを認証部14cに入力させる。そして認証部14cにある関数[E21]では、入力された乱数2と無線カード10のBT-AD1とを基に単体キーKaを生成させる。この関数[E21]は、BTI/Fに内蔵されているもので、単体キーKaを生成させるためのアルゴリズムを意味するものである。

【0071】そして、関数[E21]で生成させた単体キーKaは、初期化キーKinとの排他的論理和をして、その結果を携帯電話機20へと送信する。その後、携帯電話機20では、無線カード10から送信された単体キーKaと初期化キーKinとの排他的論理和に、更に、携帯電話機20で生成させた初期化キーKinとの排他的論理和をして単体キーKaを算出する。これにより、無線カード10と携帯電話機20との間で共通の単体キーKaを所有させることができる。

【0072】この単体キーKaを生成させるためのフローについて図11を参照しながら説明する。同図に示すように、先ず、認証部14c及び認証部24cは、それぞれの無線カード10及び携帯電話機20にあるRAM13及びRAM23から初期化キーKin、乱数2及び無線カード10のBT-ADを読み込む(S210a、S201b)。尚、携帯電話機20は、無線カード10との間で行われる通信接続の段階で無線カード10のBT-ADを既に取得している。

【0073】そして、無線カード10の認証部14cが、乱数2と、無線カード10のBT-ADとに基づいて関数[E21]で単体キーKaを生成させる(S202a)。そして、その生成された単体キーKaと、予め無線カード10が生成させた初期化キーKinとの排他的論理和((Ka XOR Kin);ここで"XOR"は排他的論理和を示すものとする(以下同様に扱う))を無線カード10から携帯電話機20へと送信する(S203a)。そして、認証部14cで生成された単体キーKaは、RAM13に格納させる(S204a)。

【0074】一方、単体キーKaと初期化キーKinとの排他的論理和を無線カード10から受信した携帯電話機20は、その受信した単体キーKaと初期化キーKinと、携帯電話機20側で生成させた初期化キーKinとの排他的論理和((Ka XOR Kin) XOR Kin)をする。この排他的論理和((Ka XOR Kin) XOR Kin)により、単体キーKaを算出させる。そして、その算出された単体キーKaはRAM23に格納させる(S204b)これにより、無線カード10と携帯端末機20との間で、共通の単体キーKaを保有させることができる。また、携帯電話機20側では、乱数を発生させないで単体キーKaを生成させることができるので、認証が完了するまでの時間を幾分節約す

14

ることができる。

【0075】次に、複合キーKabの生成について図面を参照しながら説明する。図12は、複合キーKabを生成するまでのブロック図を示したものである。図13は、複合キーKabを生成するまでの詳細なフロー図を示したものである。この複合キーKabは、恒久的に用いるリンクキーであり、接続対象のBTI/Fが複数ある場合には、そのBTI/Fの数だけ存在するものである。

【0076】また、初回の認証は、初期化キーKinによる認証を行うが、2回目以降は所定の条件を満たすことにより、単体キーKa又は複合キーKabによる認証を行う。この複合キーKabは、無線カード10から生成させる単体キーKaと携帯電話機20で生成させる単体キーKbとを共有させたものから構成される。

【0077】図12に示すように、無線カード10で生成させる複合キーKabは、無線カード10の単体キーKaを生成させる領域A1と、携帯電話機20の単体キーKbを生成させる領域A4と、無線カード10で発生させた乱数3と携帯電話機20で発生させた乱数4とをそれぞれ交換させることを行う領域A2及びA5と、無線カード10と携帯電話機20で各々複合キーKabを生成させる領域A3及び領域A6とから構成されるものである。

【0078】この無線カード10の単体キーKaを生成させる領域A1では、先ず、無線カード10で任意に発生させた乱数3と無線カード10のBT-AD1とを認証部14cへと入力させる。そして、認証部14cにある関数[E21]は、乱数3と無線カード10のBT-AD1とに基づいて単体キーKaを生成させる。

【0079】一方、携帯電話機20の単体キーKbを生成させる領域A4では、先ず、携帯電話機20で任意に発生させた乱数4と携帯電話機20のBT-AD2とを認証部24cへと入力させる。そして、認証部24cにある関数[E21]は、乱数4と携帯電話機20のBT-AD2とに基づいて単体キーKbを生成させる。

【0080】また、領域A2及び領域A5では、無線カード10で発生させた乱数3と、携帯電話機20で発生させた乱数4とをそれぞれ交換させることを行う。この無線カード10から携帯電話機20へと乱数3を送信するときには、無線カード10及び携帯端末機20内で予め生成させておいた初期化キーKinと排他的論理和をとった後に携帯電話機20へと送信させる。

【0081】同様に、携帯電話機20から無線カード10へと乱数4を送信するときには、携帯電話機20及び無線カード10内で予め生成させておいた初期化キーKinとの排他的論理和をした後に無線カード10へと送信する。このように無線カード10と携帯電話機20との間で発生する乱数3と乱数4とを交換する際に、初期化キーKinとの排他的論理和を行うのは、乱数3と乱数4とを送受信する際のセキュリティレベルを高めるためである。

(9)

15

【0082】そして、領域A2では、携帯電話機20から送信された乱数4と初期化キーKinとの排他的論理和に、無線カード10で予め生成させておいた初期化キーKinとの排他的論理和を行い、乱数4を算出させる。一方、領域A5では、無線カード10から送信された乱数3と初期化キーKinとの排他的論理和に、携帯電話機20で予め生成させておいた初期化キーKinとの排他的論理和を行い、乱数3を算出させる。

【0083】また、無線カード10で複合キーKabを生成させる領域A3では、まず、認証部14cにある関数 [21] で、乱数4と携帯電話20のBT-AD2（携帯電話機20との間で行われる通信接続の段階で既に受信）に基づいて携帯電話機20の単体キーKbを生成させる。そして、関数[E21]で生成された単体キーKbと、領域A1で生成した単体キーKaとの排他的論理和をして複合キーKabを生成させる。

【0084】一方、携帯電話機20で複合キーKabを生成させる領域A6では、認証部24cにある関数 [21] で、乱数3と無線カード10のBT-AD1（無線カード10との間で行われる通信接続の段階で受信）に基づいて無線カード10の単体キーKaを生成させる。その後、その関数[E21]で生成された単体キーKaと、領域A4で生成させた単体キーKbとの排他的論理和により、複合キーKabを生成させる。

【0085】この複合キーKabにより、片方認証（単体キーKaのみ）に比べて2倍のステップ数を行うので、より高いセキュリティレベルを確保することができる。

【0086】複合キーKabを生成するまでの詳細なフローについて図13を参照しながら説明する。同図に示すように、まず、認証部14cは、RAM13から初期化キーKinと、乱数3と、無線カード10のBT-AD1とを読み込むことを行う（S301a）。一方、認証部24cは、RAM23から無線カード10と同様の初期化キーKinと、乱数4と、携帯電話機20のBT-AD2とを読み込むことを行う（S301b）。

【0087】認証部14cでは、無線カード10のBT-AD1と、乱数3に基づいて単体キーKaを関数[E21]で生成させる（S302a）。一方、携帯電話機20では、携帯電話機20のBT-AD2と、乱数4に基づいて単体キーKbを関数[E21]で生成させる（S302b）。

【0088】無線カード10は、予め所有している乱数3と初期化キーKinの排他的論理和をとり、その結果を携帯電話機20に送信する（S303a）。そして、携帯電話機20では、無線カード10から受信した乱数3と初期化キーKinとの排他的論理和に、更に、携帯電話機20が生成した初期化キーKinとの排他的論理和をして、乱数3を算出させる（S303b、S304b）。

【0089】携帯電話機20では、上記算出した乱数3と、無線カード10のBT-AD1とにより、無線カー

16

ド10と同様の単体キーKaを関数[E21]で生成させる（S305b）。そして、携帯電話機20で予め所有している乱数4と初期化キーKinとの排他的論理和を携帯電話機20から無線カード10へと送信する（S306b）。

【0090】更に、無線カード10では、携帯電話機20から受信した乱数4と初期化キーKinとの排他的論理和に、無線カード10で予め所有している初期化キーKinとの排他的論理和をして乱数4を算出させる（S304a、S305a）。そして、無線カード10は、算出された乱数4と携帯電話機20のBT-AD2に基づいて単体キーKbを関数[E21]で生成（S306a）させて、その生成された単体キーKbとS302aで生成させた単体キーKaとの排他的論理和により複合キーKabを算出させる。その後、その算出された複合キーKabをRAM13に格納させる（S308a）。

【0091】一方、携帯電話機20では、S302bとS305bとで生成された単体キーKaとKbとの排他的論理和をして、複合キーKabを算出させる（S307b）。その後、その算出した複合キーKabをRAM23に格納させる（S308b）。これにより、無線カード10と携帯電話機20との間で複合キーKabを共有させることができる。

【0092】上記リンクキーK（初期化キーKin、単体キーKa(Kb)、複合キーKab；以下これらを総称してリンクキーKとする）を用いて無線カード10と携帯電話機20との間で行われる認証について説明する。図14は、無線カード10と携帯電話機20との間で行われる片方認証を示したブロック図である。

【0093】同図に示すように、無線カード10では、内部的に発生された任意の乱数5と、無線カード10のBT-AD1と、リンクキーKとを認証部14cに入力させる。そして、認証部14cにある関数[E1]は、入力された乱数5と、無線カード10のBT-AD1と、リンクキーKとに基づいて、SRES（Signal Result）と呼ばれるパラメータを独立に算出する。

【0094】一方、携帯電話機20では、無線カード10から乱数5を受信して、無線カード10のBT-AD1と、リンクキーKとを認証部24cに入力させる。そして、認証部24cにある関数[E1]は、入力された乱数5と、無線カード10のBT-AD1と、リンクキーKとに基づいて、SRESと呼ばれるパラメータを独立に算出する。そして、関数[E1]で算出されたSRESのパラメータを無線カード10へと送信する。

【0095】尚、携帯電話機20で所有される無線カード10のBT-AD1は、無線カード10と携帯電話機20との間で行われる問い合わせ（Inquiry）処理及び呼び出し（Page）処理により、既に取得しているものである。

【0096】その後、認証部14cでは、無線カード1

(10)

17

0で生成させたSRES'と携帯電話機20で生成させたSRESとを比較し一致しているか否かの認証を行う。そして、無線カード10のSRES'と携帯電話機20のSRESが一致しているという判断をした場合には、無線カード10から携帯電話機20を動作させるための動作信号を送信し、その動作信号を受信した携帯電話機20は、携帯電話機20を稼働させる(詳述は後述する)。

【0097】リンクキーKを用いて無線カード10と携帯電話機20との間で行われる片方認証の詳細なフローについて説明する。図15は、無線カード10と携帯電話機20との間で行われる片方認証のフローについて示したものである。

【0098】同図に示すように、先ず、認証部14c及び認証部24cは、それぞれRAM13及びRAM23から初期化キーKinと、乱数5と、無線カード10のBT-AD1とを読み込むことを行う(S401a、401b)。

【0099】そして、無線カード10は、無線カード10の乱数5を携帯電話機20へ送信する(S402a)。そして、無線カード10から乱数5を受信した携帯電話機20では、その受信した乱数5と、無線カード10のBT-AD1と、リンクキーKとに基づいてSRESを関数[E22]で生成させる(S402b、S403b)。そして、携帯電話機20は、その生成されたSRESを無線カード10に送信する(S403b)。

【0100】その後、無線カード10では、携帯電話機20からSRESを受信(S404a)し、その携帯電話機20のSRESと無線カード10で生成したSRES'とを比較して両者が一致しているか否かの判断を行う(S405a)。そして、両者が一致している場合には、認証部14cは、例えば、携帯電話機20の動作を続行(又は始動)させるための動作信号を送信する(詳述は後述する)。

【0101】そして、その動作信号を無線カード10から受信した携帯電話機20は、受信した動作信号に基づいて携帯電話機20を動作させる。又は、無線カード10から動作信号を受信した携帯電話機20は、無線カード10から特定の登録情報(例えば、無線カード10を所有している者の顔写真、氏名など)を受信し、表示部25で表示さたりすることができる(詳述は後述する)。

【0102】リンクキーKを用いて無線カード10と携帯電話機20との間で行われる双方認証の詳細なフローについて説明する。図16は、無線カード10と携帯電話機20との間で行われる双方認証のフローについて示したものである。

【0103】図16に示すように、先ず、認証部14cは、RAM13からリンクキーKと、乱数5と、無線カード10のBT-AD1と、携帯電話機20のBT-AD2

18

とを読み込む(S501a)。一方、認証部24cは、RAM23からリンクキーKと、乱数6と、無線カードのBT-AD1と、携帯電話機20のBT-AD2とを読み込む(S501b)。

【0104】そして、無線カード10は、乱数5を携帯電話機20へと送信する(S502a)。そして、無線カード10から乱数5を受信した携帯電話機20は、その受信した乱数5と、予め所有している無線カード10のBT-AD1と、予め算出しておいたリンクキーKに基づいてSRES1を関数[E22]で生成させる(S502b、S503b)。

【0105】そして、携帯電話機20は、関数[E22]で生成されたSRES1を無線カード10に送信する(S504b)。一方、無線カード10では、乱数5と、無線カード10のBT-AD1と、予め算出しておいたリンクキーKに基づいてSRES1'を関数[E22]で生成させる(S503a)。

【0106】そして、無線カード10は、無線カード10で生成したSRES1'と、携帯電話機20から受信したSRES1とが一致しているか否かを認証することを行う(S504a、S505a)。その無線カード10で生成したSRES1'と携帯電話機20で生成したSRES1とが一致していれば、認証が成功(認証成功1とする)したと判断して、次のステップに進むが、もし一致していなければ、無線カード10と携帯電話機20との認証が不成立として、次のステップには進めない。

【0107】その後、無線カード10では、携帯電話機20から乱数6を受信(S506b)し、その受信した乱数6と、リンクキーKと、携帯電話機20のBT-AD2に基づいてSRES2'を関数[E22]で生成させる(S507a)。そして、無線カード10は、その生成されたSRES2'を携帯電話機20へと送信する(S508a)。

【0108】一方、携帯電話機20では、リンクキーKと、携帯電話機20のBT-AD2と、乱数6に基づいてSRES2をアルゴリズムE22で生成させる(S506b)。そして、携帯電話機20は、無線カード10からSRES2'を受信し、その受信したSRES2'と上記生成したSRES2とを比較して一致しているか否かを認証する(S507b、S508b)。そして、その携帯電話機20で生成したSRES2と無線カード10のSRES2'とが一致していれば、認証が成功(認証成功2とする)したと判断して、次のステップに進むが、もし一致していなければ、次のステップには進まない。

【0109】そして、無線カード10と携帯電話機20との上記認証が成功(認証成功1と認証成功2)した場合には、携帯電話機20は、無線カード10から登録情報などを受信する。

(11)

19

【0110】例えば、携帯電話機20は、携帯電話機20の操作を続行（又は始動）させるための続行信号を無線カード10から受信し、その受信した続行信号に基づいて携帯電話機20を作動（詳述は後述する）させて、登録情報などを無線カード10から受信する。

【0111】前記携帯電話機20は、認証情報に基づいて動作をする電子機器である。この電子機器は、携帯電話機のみならず、パーソナルコンピュータ、自動車なども対象として含まれるものとする。本実施形態で携帯電話機20は、図5に示すように、携帯電話機20内の全体の制御を司るCPU21と、CPU21が実行する制御プログラムを格納したROM22と、無線カード10と携帯端末機20との間で認証を行うための認証情報を記録するコード情報領域23aを備えたRAM23と、無線カード10との間でデータの送受信をする通信I/F24と、データの内容を表示させる表示部25と、データを入力する操作部26とを有しているものである。

【0112】表示部25は、情報データを表示させる表示手段であり、例えば、液晶画面などが挙げられる。具体的に表示部25は、CPU21からの命令により、通信I/F24で受信した情報データを表示させる。また、無線カード10と携帯電話機20との間で適正な認証が行われた場合には、表示部25では、適正な認証が行われた旨の表示（例えば、“無線カード10との認証は終了しました”。）を行う。

【0113】操作部26は、情報データを入力し、表示部25にある画面表示を操作する操作手段であり、例えば、キーボードなどが挙げられる。尚、操作部26の形状としては、ボタン形状のものや、ジョイスティック型のものが挙げられる。

【0114】RAM23は、無線カード10と携帯端末機20との間で認証を行うための認証情報を記録するコード情報領域23aを有するものである。このコード情報としては、128ビットで構成されている任意のコードである乱数、PINコード（Personal Identification Number）、BT-ADなどが挙げられる。

【0115】また、無線カード10と携帯電話機20との間でしか情報データを交信することができないようにするためn予め格納された秘密鍵のデータ（図示せず）や、操作部26の入力操作による暗証番号（例えば“1234”などの情報）なども、コード情報として格納することができる。このコード情報により無線カード10と携帯電話機20との間で、BTなどの通信方式によるものとは異なる認証処理を行うことができるので、無線カード10と携帯電話機20の間で行われるデータ送受信の際のセキュリティレベルを上げることができる。

【0116】前記CPU21は、携帯電話機20内の全体の制御を司るものであり、本実施形態では、第二認証部の認証に基づいて電子機器を動作させる動作制御部21aと、操作手段に対する操作を検知する検知部21b

20

と、認証情報を無線カード10から取得するために、認証情報を要求する認証要求情報を生成する認証情報要求部21cとを有している。

【0117】動作制御部21aは、第二認証部（本実施形態では、認証部24c）の認証に基づいて電子機器（本実施形態では、携帯電話機20）を動作させるものである。具体的に動作制御部21aは、認証部24cにより、無線カード10と携帯電話機20との間の認証が成功した場合には、認証部24c（又は認証部14c）から携帯電話機20の動作をさせるための動作信号が入力される。

【0118】動作信号が入力された動作制御部21aは、携帯電話機20の動作を可能にするようにするために、携帯電話機20の電源部27にある電源を投入したり、又は、操作部26を使用可能状態にする。尚、動作制御部21aは、電源部27とは別の電源で動作するものであり、電源部27が稼働していなくても動作制御部21aの動作が可能である。

【0119】検知部21bは、操作部26に対する操作を検知するものである。具体的に検知部21bは、操作部26の操作により発生された電流パルス、電圧パルスなどを検知するものである。そして、操作部26の操作を検知した検知部21bは、その検知した信号に基づいて、無線カード10に対して認証情報を要求するための要求信号を認証情報要求部21cへと出力させる。

【0120】認証情報要求部21cは、認証情報を無線カード10から取得するために、認証情報を要求する認証要求情報を生成するものである。具体的に認証情報要求部21cは、検知部から要求信号が入力された場合には、無線カード10に対して認証情報を要求するための認証要求情報を生成する。

【0121】そして、認証情報要求部21cは、その生成した認証要求情報を送信部24aを介して無線カード10へと送信させる。その後、認証要求情報を取得した無線カード10は、認証部14cで認証情報を生成させて、その生成した認証情報を携帯電話機20へと送信し、その認証情報を受信した認証部24cでは、受信した認証情報に基づいて認証を行う。

【0122】前記通信I/F24は、無線カード10にある通信I/F14との間でデータの送受信をするものであり、例えば、BT、IrDAなどが挙げられる。本実施形態で通信I/F24は、認証情報を要求する認証要求情報を無線カード10に対して送信する送信手段を有する送信部24aと、認証情報などを無線カードから受信する受信手段を有する受信部24bと、受信手段が無線カード10から受信した認証情報に基づいて無線カード10の認証を行う第二認証部を有する認証部24cとを有している。

【0123】送信部24aは、受信手段（本実施形態では、無線カード10の受信部14b）に対して、前記受

10

20

30

40

50

(12)

21

信手段の周波数とクロックのタイミングにより、前記受信手段を呼び出し、その呼び出しに応じた前記受信手段と通信接続をした後に前記認証情報又は前記認証要求情報を送信する送信手段である。この送信部24a-受信部14bと送信部14a-受信部24b間で行われる通信接続は、本実施形態では、BTを用いて行うものとする。

【0124】このBTは、通信可能な範囲内にある無線カード10との接続可能性の向上等のために、待ち受け側のBTが接続要求を監視する周波数（待ち受け周波数）を所定時間毎に変化させている。

【0125】この待ち受け周波数の変化パターンは、待ち受け側のBTに割り当てられた識別情報（BT-AD（address）、BT-CLK（Clock））によって異なるが、通常、通信を開始しようとするときには、通信可能な範囲内に存在するBTの識別情報（特にBT-AD）が不明である。このため、通信を開始しようとする送信部24aは、まず、周囲のBTを検出するための問い合わせ（Inquiry）処理によって、自機の周囲に存在するBTを検出する。

【0126】このInquiryの要求に応じて、周囲のBTからの応答を受信部24bで受信すると、この応答中のBT-ADに応じて通信しようとするBTを選択し、呼び出し（Page）処理によって、選択した相手方を呼び出す。このPageにより、相手側のBT送受信機が提供しているサービスを検出すると、所定のサービスを指定して、通信接続モードに移行し、接続を確立する。

【0127】この通信接続では、無線カード10と携帯電話機20との間でデータのパケットの送受信は行われない。また、無線カード10と携帯電話機20との間で通信接続が確立した後に、携帯電話機20にある送信部24a・受信部24bと無線カード10にある送信部14a・受信部14bとの間で認証情報が送受信されて、認証部14c及び認証部24cで認証が行われる。

【0128】認証部24cは、無線カード10で生成された認証情報と携帯電話機20で生成された認証情報とが一致しているか否かを判断するものである。この認証部24cで行う認証は、上述の通信I/F14と同様に、無線カード10との間で通信接続が確立された後に行われるものである。

【0129】この認証部24cで行われる認証は、認証部14cと同様の動作をするものであり、リンクキーという概念で管理されている。また、認証は、無線カード10をマスター、携帯電話機20をスレーブとして、ピコネットを形成してから行われ、この認証が成功したときのみ携帯電話機20の使用が可能となる。

【0130】ここで用いられるBTのリンクキーとしては、主に初期化キーKin、単体キーKa、複合キーKabがあり、それぞれ128ビットの固有長を有する。このリンクキーの生成とそのリンクキーを用いた認証方法は、

22

上記無線カード10における認証部14cと同様の方法で行われる（図8から図16を参照）。

【0131】この認証部24cでは、無線カード10と携帯電話機20との間の認証が成功したと判断した場合には、携帯電話機20を動作させるための動作信号を動作制御部21aへと出力させる。また、認証部24cは、無線カード10の認証部14cから通信I/F14（24）を介して携帯電話機20を作動させるための動作信号を受け取ることもできる。

【0132】（機器認証システムを用いた機器認証方法）上記構成を有する機器認証システムによる機器認証方法は、以下の手順により実施することができる。図17は、本実施形態に係る機器認証方法の手順を示すフロー図である。

【0133】同図に示すように、まず、無線カード10を使用したい携帯電話機20に近づけるステップを行う（S601）。次いで、無線カード10と携帯電話機20との間の通信接続を確立させるステップと行う（S602）。具体的に、無線カード10に複数の携帯電話機20の認証情報が格納されている場合には、利用者が操作部10を介して、使用したい携帯電話機20の認証情報を選択し、その選択された認証情報に対応する携帯電話機20と通信接続を行う。

【0134】次いで、無線カード10と携帯電話機20との間の認証を行う（S603）。具体的に、無線カード10と携帯電話機20との間で通信接続が確立した場合には、無線カード10にある認証部14dと携帯電話機20にある認証部24dとの間で、認証情報に基づいて上述した認証を行う。

【0135】次いで、無線カード10と携帯電話機20との間の認証が成功したか否かの判断を行うステップをする（S604）。具体的には、無線カード10と携帯電話機20との間で通信接続が確立した後に、無線カード10にある認証部14dと携帯電話機20にある認証部24dは、認証情報（初期化キーKin、単体キーKa、又は、複合キーKab）を各自生成させて、その認証情報により認証を行う。

【0136】また、この認証情報は、携帯電話機20にある操作部26の操作により認証情報を無線カード10に対して要求することができる。具体的には、操作部26の操作を検知部21bが検知し、その操作部26の操作を検知した検知部21bは、その検知した信号に基づいて、無線カードに対して認証情報を要求するための要求信号を認識情報要求部21cへと出力させる。

【0137】そして、認証情報要求部21cは、検知部から要求信号が入力された場合には、認証情報を無線カード10に対して要求するための認証要求情報を生成する。そして、送信部24aは、その生成した認証要求情報を無線カード10へと送信させる。その後、認証要求情報を取得した認証部14cは、認証情報を生成させ

(13)

23

て、その生成した認証情報を携帯電話機20へと送信させる。その後、認証情報に基づいて、携帯電話機20にある認証部24cと無線カード10にある認証部14cで認証を行う(図8～図16参照)。

【0138】次いで、無線カード10と携帯電話機20との間の認証が成功した場合には、携帯電話機20を動作させるステップを行う(S605)。具体的には、無線カード10にある認証部14dと携帯電話機20にある認証部24dとの間で認証が成功したと判断した場合には、認証部14dが携帯電話機20の動作をさせるための続行信号を携帯電話機20へと送信する。

【0139】そして、無線カード10から動作信号を受信した通信I/F24は、その動作信号を動作制御部21aへと入力させる。その後、通信I/F24から動作信号が入力された動作制御部21aは、携帯電話機20を動作させるために、電源部27を稼働させて電源を投入させたり、又は、操作部26を使用可能状態にする。

【0140】また、無線カード10と携帯電話機20との間で通信接続が確立され、認証が成功したときには、認証部24cが携帯電話機20を動作させるための続行信号を動作制御部21aへと出力させることもできる。一方、無線カード10と携帯電話機20との間の認証が成功しない場合には、携帯電話機20を動作させないステップを行う(S606)。具体的には、無線カード10にある認証部14dと携帯電話機20にある認証部24dとの間で認証が成功しない場合(例えば、無線カード10と携帯電話機20とが遠く離れており通信できない場合には、認証できない)には、認証部14dが携帯電話機20の動作を続行させない(又は、始動停止)ようにするための動作拒否信号を携帯電話機20へと送信する。そして、無線カード10から続行拒否信号を受信した携帯電話機20は、携帯電話機20を続行させないようにするために電源の供給を切断したり、又は、操作部26を使用不可状態にする。

【0141】その後、無線カード10と携帯電話機20との間の認証が成功したかの判断を行う(S607)。次いで、無線カード10と携帯電話機20との間で認証が成功した場合には、携帯電話機20を操作させるステップを行う(S608)。これにより、無線カード10を持った利用者が、携帯電話機20の通信可能範囲内に入り再び無線カード10と携帯電話機20との間で認証処理を行った結果、この認証に成功すれば、携帯電話機20を動作させることができる。

【0142】(機器認証システム及び機器認証方法による作用及び効果)このような本実施形態に係る機器認証システムによれば、無線カード側で生成された電子機器の動作を制御するための認証情報を電子機器が取得することにより、その取得した認証情報に基づいて電子機器を動作させることができる。

【0143】そのため、電子機器で取得した認証情報が

24

適正な情報でない場合には、前記電子機器を作動させないようにすることができ、適正な認証情報を持った者のみが電子機器を作動させることができる。また、電子機器は、無線カード(適正な認証情報が格納されたもの)を有する者のみしか使用できないことになるので、前記電子機器のみを盗難されたり、又は、紛失した場合であっても、その盗難した者等によって不当に使用されることがなくなる。

【0144】特に、本実施形態では、電子機器に操作部26が設けられているので、その操作部26を操作させることにより、無線カードに対して電子機器を作動させるための認証情報を要求することができる。そのため、電子機器の通信可能範囲内に無線カードがあれば、無線カードを持ち歩かなくても電子機器を作動させる認証情報を無線カードから容易に取得することができる。

【0145】また、送信手段は、受信手段に対して、その受信手段が有する特定の周波数とクロックのタイミングにより受信手段との間で通信接続を確立させることができるので、例えば、近接無線通信を行うBTを用いて認証を行うことができる。

【0146】また、本実施形態に係る機器認証方法によれば、電子機器は、無線カード側から電子機器を制御するための認証情報を取得することができるので、その認証情報に基づいて電子機器を動作させることができる。

【0147】(第1変更例)尚、本発明は上記実施形態に限定されるものではなく、本変更例では図18に示すように、認証情報要求部21cに認証要求情報を所定時間毎に要求するための時間を設定する設定部21dと、設定部21dで設定された時間を解除する解除部21eとを設けてもよい。図19は、本変更例1に係る機器認証システムの概略構成を示したものである。

【0148】同図に示すように、パーソナルコンピュータ20にある設定部21dで設定された時間毎に無線カード10は、乱数7(又は乱数8)を送信し、その乱数7(又は乱数8)を送信したことによる応答1(又は応答2)をパーソナルコンピュータ20から受信し、その受信した応答1(又は応答2)に基づいて認証を行い、パーソナルコンピュータ20の動作の続行の可否を行うことを示したものである。

【0149】設定部21dは、認証情報要求部21cに認証要求情報を所定の時間毎に要求するための時間を設定する設定手段である。具体的には、利用者が操作部26を用いて認証要求情報を要求する時間を設定し、その設定された時間信号を設定部21dへと出力させる。

【0150】そして、操作部26から時間信号が入力された設定部21dは、その設定した時間が経過した場合には、無線カード10と認証を行うようにするための認証命令信号を認証部24cに出力する。そして、設定部21dから認証命令信号が入力された認証部24cは、無線カード10との間で認証を行う。

(14)

25

【0151】解除部21eは、設定部21dで設定された要求時間を解除するものである。具体的には、利用者が操作部26を用いて、設定された要求時間を解除するための操作をして、その要求時間を解除するための信号を解除部21eへと出力させる。そして、その設定時間を解除するための信号が入力された解除部21eは、設定部21dで設定された要求時間を解除する。

【0152】上記構成を有する本変更例における認証の方法は、以下の手順により実施することができる（図示せず）。まず、使用者がパーソナルコンピュータ20の操作部16を介して無線カード10の認証を行う時間を設定するステップを行う。具体的には、利用者が、操作部26の操作キーを入力してパーソナルコンピュータ20が無線カード10を定期的に認証する時間を設定し、その設定した信号（要求信号）を設定部21dへと入力させる。

【0153】次いで、設定部21bで設定された要求時間が経過した場合には、無線カード10との間の認証を行うステップを行う。具体的に、操作部26から要求信号が入力された設定部21bは、その設定された要求時間が経過した場合には、無線カード10と認証を行うようにするための認証命令信号を認証部24cに出力する。そして、設定部21dから認証命令信号が入力された認証部24cは、無線カード10との間の認証を行う。

【0154】その後、認証部24cで無線カード10との間で認証が成功したときには、パーソナルコンピュータ20の使用を続行させるステップを行う。一方、認証部14eでパーソナルコンピュータ20との認証が失敗したときには、パーソナルコンピュータ20の使用を続行させないステップを行う。

【0155】具体的に、認証部24cで無線カード10との間で認証が成功した場合には、認証部24cは、パーソナルコンピュータ20を続行させるための続行信号を動作制御部21aに出力する。その続行信号が入力された動作制御部21aは、パーソナルコンピュータ20をそのまま続行させる。

【0156】一方、認証部24cは、無線カード10との間で認証が成功しなかった場合には、パーソナルコンピュータ20の動作を停止させるための続行拒否信号を動作制御部21aへと出力する。そして、続行拒否信号が認証部24cから入力された動作制御部21aは、パーソナルコンピュータ20の動作を続行させないようにするために、電源部27にある電源を切断したり、又は、操作部26で操作することができないようにする。

【0157】これにより、パーソナルコンピュータ20は、無線カード10を所持している利用者がパーソナルコンピュータ20から遠ざかってしまい無線カード10との間の認証に失敗したときには使用不可とさせることができる。そのため、無線カード10を所持している利

26

用者がパーソナルコンピュータ20に近づいている時だけ、パーソナルコンピュータ20を使用することができる。

【0158】また、無線カード10を所持している利用者がパーソナルコンピュータ20から離れてしまった場合には、パーソナルコンピュータ20を稼働させないようにすることができるので、第三者に使用させないようにすることができる。そのため、パーソナルコンピュータ20に格納されている情報の機密性を高めることができる。

【0159】（変更例2）また、複数の無線カード10がある場合に、それらの無線カード10が有する認証情報（BTのBT-AD(address)、BT-CLK(clock)、リンクキーKなど）を格納する統合手段（図示せず）を無線カード10に設けてもよい。図20は、本変更例における機器認証システムの概略構成図を示したものである。

【0160】同図に示すように、本変更例に係る機器認証システムは、無線カード10a～10cに対応する携帯電話機20aと、パーソナルコンピュータ20bと、自動車20cとに含まれる各認証情報（各機種のBT-AD20a～20c、リンクキーK1～K3）を1つの無線カード10に統合したものである。

【0161】また、同図より、この無線カード10を自動車（内部に設置されている機器も含む）のキーとしても用いることができる。これにより、無線カード10とBTを搭載した自動車の組み合わせで、ドアの開閉や、エンジンの起動や、カーナビゲーションの操作をすることができる。この場合、無線カード10を紛失したときには、先に述べたように、無線カード10を販売店で再購入し、特定のPINコードなどを改めて設定することで、再びその自動車におけるキー（無線カード10）又は免許証として用いることができる。

【0162】統合は、複数の無線カード10が有する識別情報を格納することによって実現する。例えば、メモリカードなどが挙げられる。具体的に統合手段は、図21に示すように、無線カード10bの内部に存在するSDメモリーカードインターフェース（図示せず）に他の無線カード10a及び10cを接続し、その接続した他の無線カード10a及び10cのBT-AD20a及び20cとリンクキーK1及びK3とを格納する。

【0163】また、各無線カード10が所有している識別情報をBTを介して統合手段に格納する場合には、例えば、無線カード10bがマスターとなって、他の無線カード10a及び10cがスレーブとなるようなピコネットを形成させる。尚、このピコネットに属する無線カード10a～10cには、それぞれ異なったのPINコード（PIN1～3）が設定されている。

【0164】そして、これらのPIN1～3をベースとして、マスターである無線カード10bとスレーブであ

(15)

27

る無線カード10a又は10cとの間でそれぞれ通信接続を確立させ、マスターの無線カード10bにある統合手段にスレーブの無線カード10a又は10cが有するそれぞれのBT-AD、リンクキーKを格納させる。

【0165】これにより、複数の電子機器が有するそれぞれの認証情報(PINコードなど)を1つの無線カード10bが所有しているため、この無線カード10bで複数の電子機器の動作を制御することができる。

【0166】無線カード10は、1つの認証情報で複数の電子機器を制御するための情報を格納することもできる。例えば、図22に示すように、無線カード10に携帯電話機20aと、パーソナルコンピュータ20bと、自動車20cにそれぞれ同一のPINコードを設定する。そして、そのPINコードを無線カードにある統合手段に格納する。これにより、無線カード10は、統合手段が所有しているPINコードと同一のPINコードを所有している電子機器の動作制御を行うことができる。尚、各無線カード10が所有する識別情報の統合は、識別情報を管理するホストシステム30で行うことができる。

【0167】これにより、携帯電話機20aと、パーソナルコンピュータ20bと、自動車20cに対応するそれぞれのPINコードを用意する必要がないので、製造工場で複数のPINコードを管理する必要がなくなる。

【0168】(変更例3) また、所定の時間帯において、無線カード10に対して認証要求情報を要求する頻度を設定する時間帯設定部(図示せず)を通信I/F21に設けてもよい。

【0169】時間帯設定部は、所定の時間帯において、無線カード10に対して認証要求情報を要求する頻度を設定するものである。具体的には、まず、利用者が操作部26を操作させることにより、無線カード10に対して認証要求情報を要求する特定の時間帯と、その特定の時間帯内で無線カード10に対して認証要求情報を要求する回数を入力する。

【0170】例えば、電子機器20の利用者が午前の10時から12時までの間に電子機器20を使用する頻度が高ければ、利用者が所有する無線カード10と電子機器20との間の認証の回数(5分ごとなど)を多くし、一方、電子機器20を利用する頻度が低い時間帯である午後7時から8時までの間は、電子機器20と利用者が所有する無線カード10との間で行う認証の回数を少なくする(15分ごとなど)。

【0171】そして、操作部26から認証情報を要求する特定の時間帯と、その特定の時間帯内で無線カード10に対して認証情報を要求する回数が入力された時間帯設定部は、その設定された特定の時間帯と、その特定の時間帯内で無線カード10に対して要求する回数とに基づいて、認証情報を要求するための要求信号を認証情報要求部21cに出力する。

28

【0172】そして、時間帯設定部から要求信号が入力された認証情報要求部21cは、認証情報を要求するための認証要求情報を生成し、その生成された認証要求情報を無線カード10に対して送信する。その後、携帯電話機20から認証要求情報を無線カード10は、認証部14cで認証情報を生成させて、その生成された認証情報により無線カード10と携帯電話機20との間で認証を行う。そして、無線カード10と電子機器20との間で認証が成功した場合には、電気機器20の使用が可能となる。

【0173】これにより、時間帯設定部で設定された時間帯で電子機器20と無線カード10との間の認証を行う頻度を設定することができるので、電子機器20を使用する頻度の高い時間帯に、電子機器20と無線カード10との間で認証を行う回数を多くすることができる。

【0174】そのため、電子機器20を使用する頻度の高い時間帯には、電子機器20と無線カード10との間の認証を通常よりも多く行うことができるので、無線カード10を所持する利用者が電子機器20から少しの間離れたとしても、その間の電子機器の動作を停止することができ、電子機器20に格納されている情報を第三者に盗用されることがなくなる。

【0175】

【発明の効果】以上説明したように本発明の機器認証システム及び機器認証方法によれば、電子機器を使用する際に、利用者の無線カードにより認証を行わなければ、その電子機器を使用することができないので、ユーザの電子機器(例えば、携帯端末機)が盗難等されたとしても第三者に不正に使用されることがなくなる。また、無線カード内にある特有の認証情報により認証を行うので、第三者に容易に認証情報を解読させないようにすることができる。

【図面の簡単な説明】

【図1】本発明の実施形態に係る機器認証システムの概略構成を示すブロック図である。

【図2】本実施形態における無線カードと携帯電話機との間で行われる片方向認証を示した図である。

【図3】本実施形態における無線カードと携帯電話機との間で行われる相互認証を示した図である。

【図4】本実施形態における無線カードと携帯電話機との間の認証をBTを用いて行ったことを示した図である。

【図5】本実施形態における機器認証システムの内部構成を示したブロック図である。

【図6】本実施形態における無線カードと携帯電話機との間の認証で用いられるコード情報を示したものである。

【図7】本実施形態におけるホストシステムで管理されている携帯電話機のPINコードを示したものである。

【図8】本実施形態における無線カードと携帯電話機と

(16)

29

の間で認証する際に用いられる初期化キーKinが生成されるまでのブロック図を示したものである。

【図9】本実施形態における無線カードと携帯電話機との間で認証する際に用いられる初期化キーKinが生成されるまでの過程を示したフロー図である。

【図10】本実施形態における無線カードと携帯電話機との間で認証する際に用いられる単体キーKaが生成されるまでのブロック図を示したものである。

【図11】本実施形態における無線カードと携帯電話機との間で認証する際に用いられる単体キーKaが生成されるまでの過程を示したフロー図である。

【図12】本実施形態における無線カードと携帯電話機との間で認証する際に用いられる複合キーKabが生成されるまでのブロック図を示したものである。

【図13】本実施形態における無線カードと携帯電話機との間で認証する際に用いられる複合キーKabが生成されるまでの過程を示したフロー図である。

【図14】本実施形態における無線カードと携帯電話機との間で行われる片方認証を示したブロック図である。

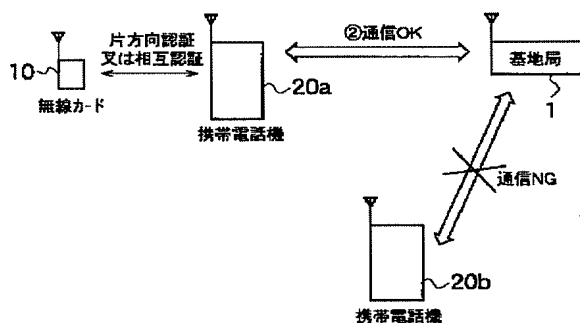
【図15】本実施形態における無線カードと携帯電話機との間で行われる片方認証を示したフロー図である。

【図16】本実施形態における無線カードと携帯電話機との間で行われる相互認証を示したフロー図である。

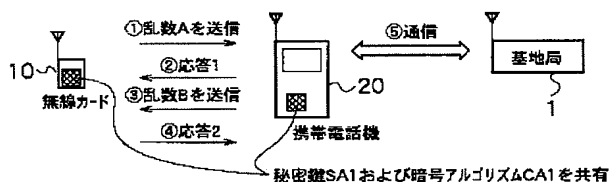
【図17】本実施形態における機器認証方法を示したフロー図である。

【図18】第1変更例に係る機器認証システムの概略構成を示した図である。

【図1】



【図3】



30

【図19】第1変更例に係る機器認証システムの内部構造を示したブロック図である。

【図20】第2変更例に係る機器認証システムの概略構成を示した構成図である。

【図21】第2変更例における複数の無線カードにある認証情報を1つの無線カードに統合した図を示したものである。

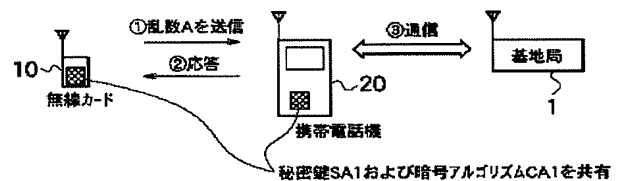
【図22】第2変更例における無線カードで複数の電子機器と認証を行っていることを示した図である。

【図23】従来におけるパスワードでの認証を示した図である。

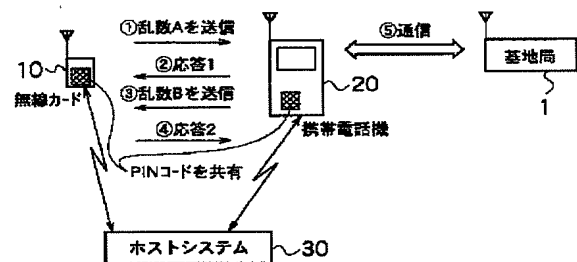
【符号の説明】

1…基地局、10 (10a～10c) …無線カード、11…CPU、12…ROM、13…RAM、13a…コード情報領域、14…通信I/F、14a…送信部、14b…受信部、14c…認証部、15…表示部、16…操作部、20 (20a～20c) …携帯電話機/パーソナルコンピュータ/自動車、21…CPU、21a…動作制御部、21b…検知部、21c…認識情報要求部、21d…設定部、21e…解除部、22…ROM、23…RAM、23a…コード情報領域、24…通信I/F、24a…送信部、24b…受信部、24c…認証部、25…表示部、26…操作部、27…電源部、30…ホストシステム、31…CPU、32…ROM、33…RAM、34…通信I/F、35…記憶装置、36…操作部、37…表示部

【図2】

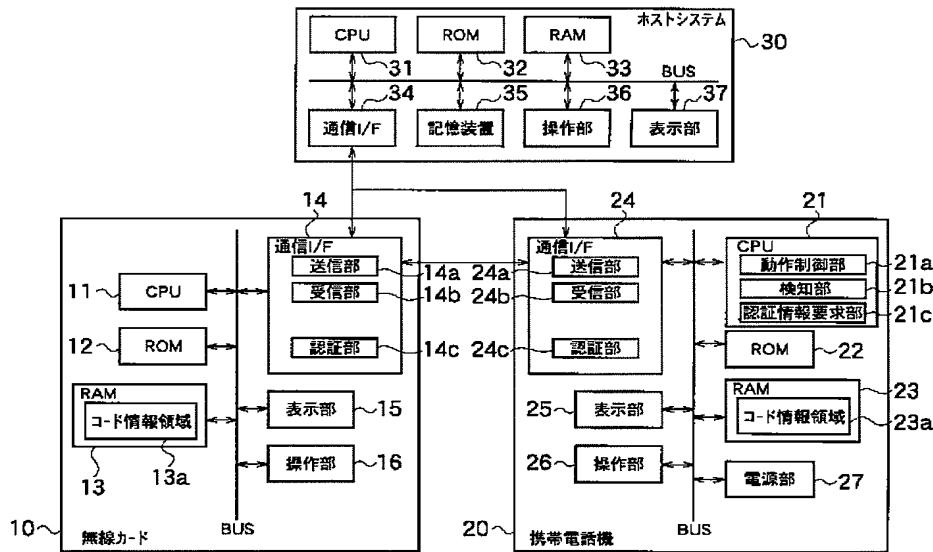


【図4】



(17)

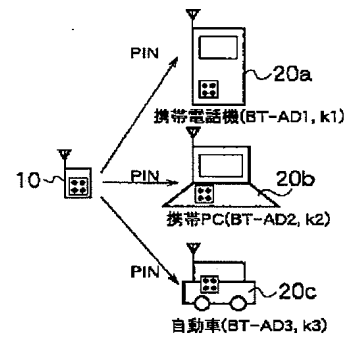
【図5】



【図6】

| コード情報 |
|--------------------|
| 乱数 (128ビット) |
| PINコード, PINコード長 |
| 暗証番号 (例えば, "1234") |

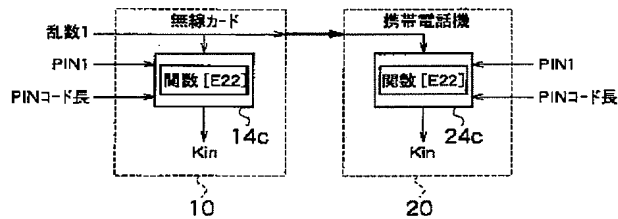
【図22】



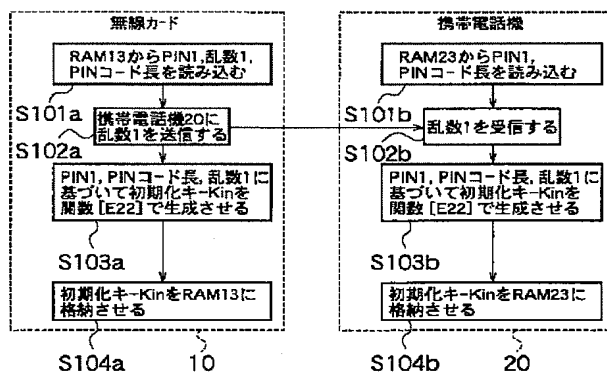
【図7】

| 端末機情報 | |
|--------|------|
| 携帯端末機1 | PIN1 |
| 携帯端末機2 | PIN2 |
| 携帯端末機3 | PIN3 |
| ... | ... |
| 携帯端末機n | PINn |

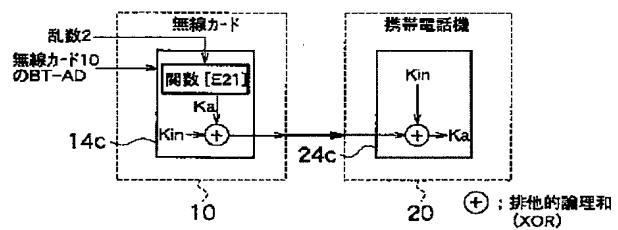
【図8】



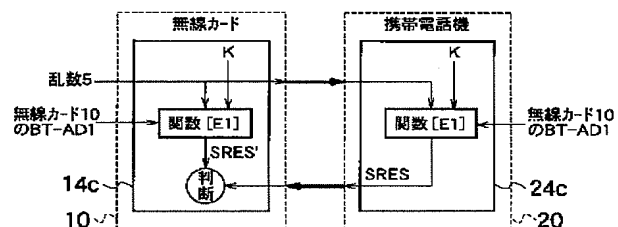
【図9】



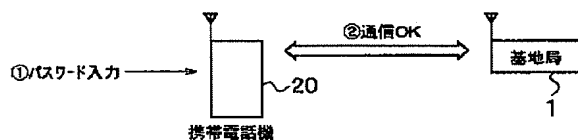
【図10】



【図14】

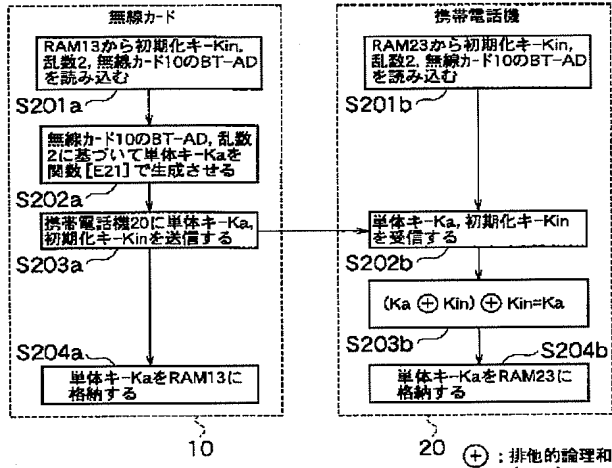


【図23】

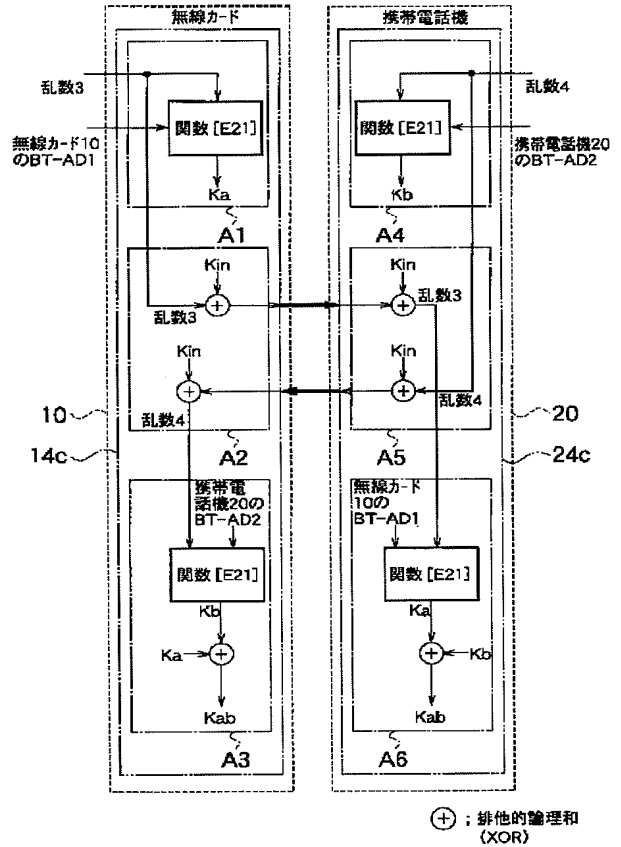


(18)

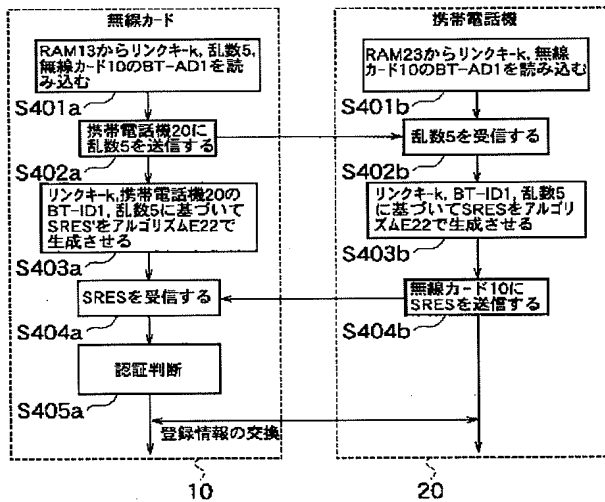
【図11】



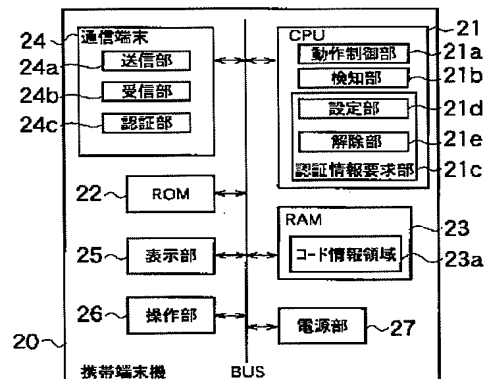
【図12】



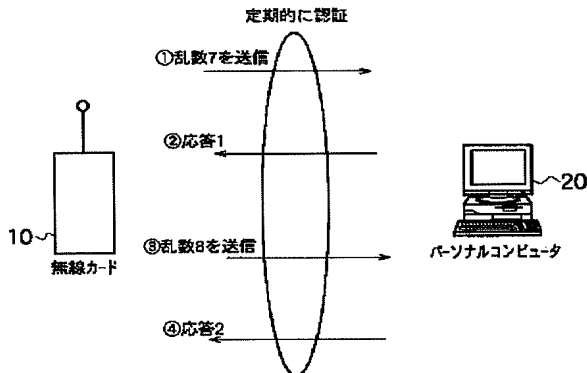
【図15】



【図18】

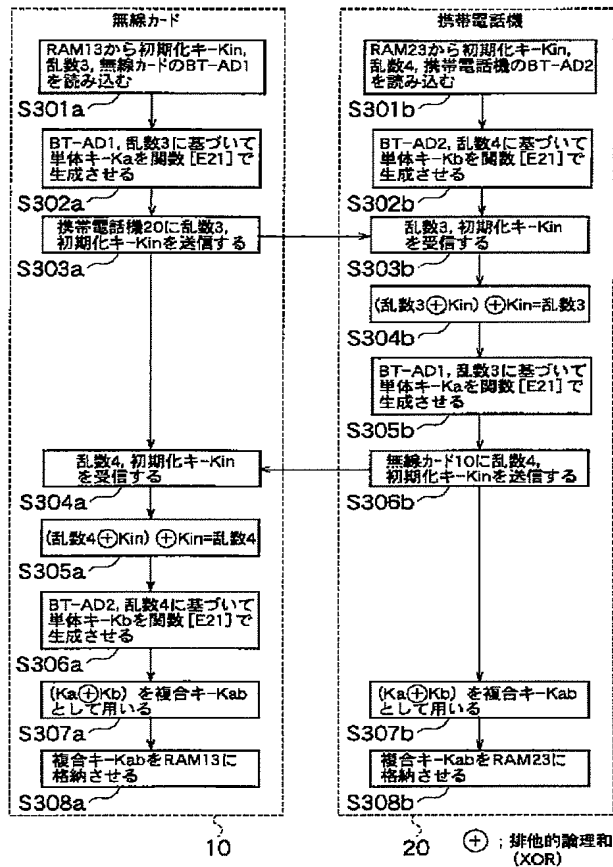


【図19】

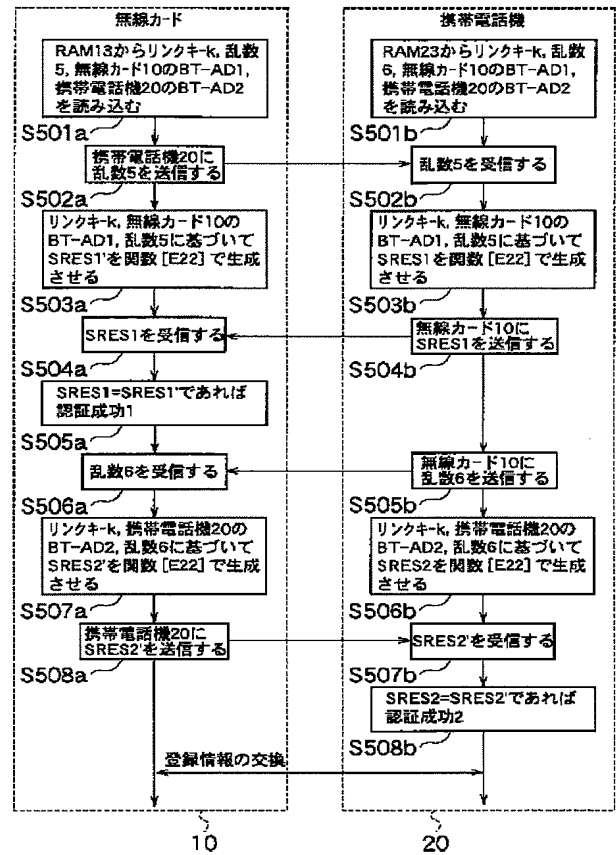


(19)

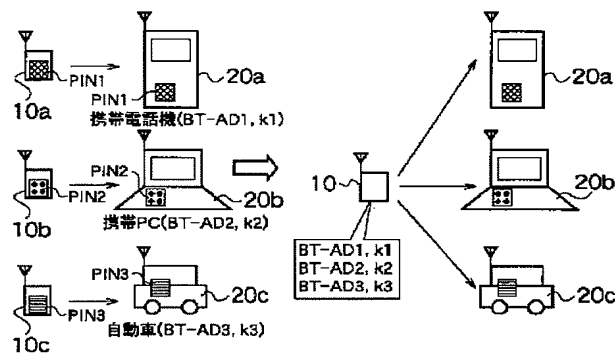
【図13】



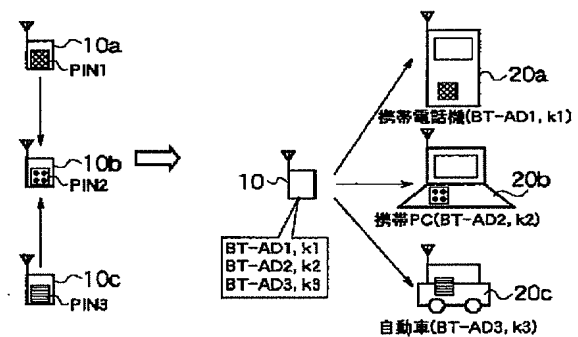
【図16】



【図20】

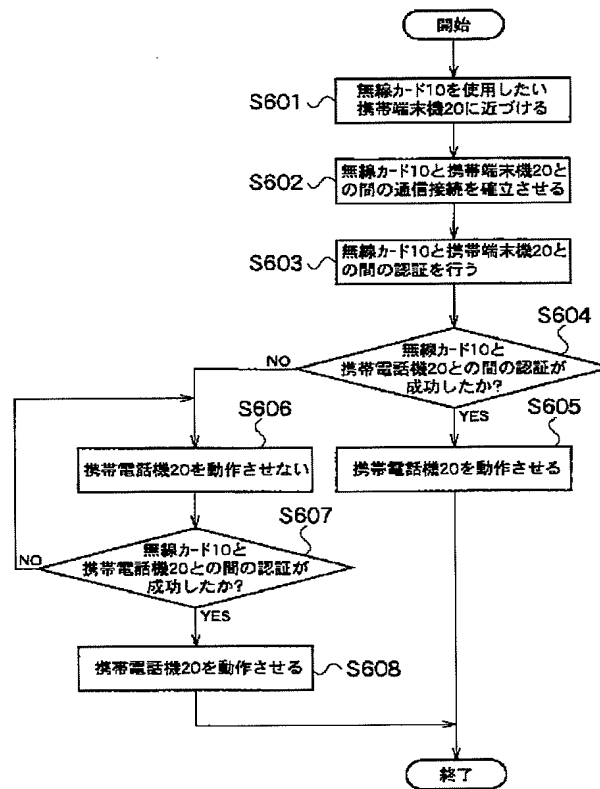


【図21】



(20)

【図17】



フロントページの続き

Fターム(参考) 5B085 AC12 AE09 AE12

5J104 AA04 AA07 KA02 KA04 KA15
NA02 PA025K067 AA32 BB04 CC04 CC08 CC10
DD17 EE02 EE10 FF23 HH21
HH22 HH23 HH36 KK13 KK15